

Amendments to the Claims

Claims 1 - 7 (canceled)

1 Claim 8 (previously presented): A computer program product for providing end-to-end user
2 authentication for legacy host application access, said computer program product embodied on a
3 computer-readable medium readable by a computing device in a computing environment and
4 comprising:

5 computer-readable program code means for establishing a secure session from a client
6 machine to a server machine using a digital certificate transmitted from said client machine to said
7 server machine, wherein said digital certificate represents said client machine or a user thereof;

8 computer-readable program code means for storing said transmitted digital certificate at
9 said server machine;

10 computer-readable program code means for establishing a session from said server
11 machine to a host system on behalf of said client machine, responsive to establishment of said
12 secure session, using a legacy host communication protocol;

13 computer-readable program code means for automatically sending a log-on message from
14 said client machine to said server machine, responsive to receiving, at said client machine, a
15 request from said host system for log-on information of said user, wherein said log-on message
16 uses placeholder syntax in place of a user identifier and a password of said user;

17 computer-readable program code means for passing said stored digital certificate from
18 said server machine to a host access security system, responsive to receiving, at said server

Serial No. 09/466,625

-4-

Docket RSW990077

19 machine, said log-on message from said client machine;

20 computer-readable program code means, operable in said host access security system, for
21 using said passed digital certificate to locate access credentials for said user;

22 computer-readable program code means for returning, from said host access security
23 system to said server machine, a user identifier associated with said located access credentials and
24 either a stored password or a generated password substitute representing said located credentials;

25 computer-readable program code means for modifying, by said server machine, said
26 received log-on message by replacing said placeholder syntax with said returned user identifier
27 and password or password substitute; and

28 computer-readable program code means for forwarding said modified log-on message
29 from said server to said host system as a response to said request for log-on information, such
30 that said user identifier and password or password substitute from said forwarded log-on message
31 can be used by said host system to transparently log said user on to a secure legacy host
32 application executing at said host system, without requiring change to said host system.

Claims 9 - 16 (canceled)

1 Claim 17 (previously presented): A system for providing end-to-end user authentication for
2 legacy host application access in a computing environment, comprising:

3 means for establishing a secure session from a client machine to a server machine using a
4 digital certificate transmitted from said client machine to said server machine, wherein said digital

Serial No. 09/466,625

-5-

Docket RSW990077

5 certificate represents said client machine or a user thereof;

6 means for storing said transmitted digital certificate at said server machine;

7 means for establishing a session from said server machine to a host system on behalf of
8 said client machine, responsive to establishment of said secure session, using a legacy host
9 communication protocol;

10 means for automatically sending a log-on message from said client machine to said server
11 machine, responsive to receiving, at said client machine, a request from said host system for log-
12 on information of said user, wherein said log-on message uses placeholder syntax in place of a
13 user identifier and a password of said user;

14 means for passing said stored digital certificate from said server machine to a host access
15 security system, responsive to receiving, at said server machine, said log-on message from said
16 client machine;

17 means, operable in said host access security system, for using said passed digital certificate
18 to locate access credentials for said user;

19 means for returning, from said host access security system to said server machine, a user
20 identifier associated with said located access credentials and either a stored password or a
21 generated password substitute representing said located credentials;

22 means for modifying, by said server machine, said received log-on message by replacing
23 said placeholder syntax with said returned user identifier and password or password substitute;
24 and

25 means for forwarding said modified log-on message from said server to said host system

26 as a response to said request for log-on information, such that said user identifier and password or
27 password substitute from said forwarded log-on message can be used by said host system to
28 transparently log said user on to a secure legacy host application executing at said host system,
29 without requiring change to said host system.

Claims 18 - 25 (canceled)

1 Claim 26 (previously presented): A method for providing end-to-end user authentication for
2 legacy host application access in a computing environment, comprising steps of:
3 establishing a secure session from a client machine to a server machine using a digital
4 certificate transmitted from said client machine to said server machine, wherein said digital
5 certificate represents said client machine or a user thereof;
6 storing said transmitted digital certificate at said server machine;
7 establishing a session from said server machine to a host system on behalf of said client
8 machine, responsive to establishment of said secure session, using a legacy host communication
9 protocol;
10 automatically sending a log-on message from said client machine to said server machine,
11 responsive to receiving, at said client machine, a request from said host system for log-on
12 information of said user, wherein said log-on message uses placeholder syntax in place of a user
13 identifier and a password of said user;
14 passing said stored digital certificate from said server machine to a host access security

Serial No. 09/466,625

-7-

Docket RSW990077

15 system, responsive to receiving, at said server machine, said log-on message from said client
16 machine;

17 using, by said host access security system, said passed digital certificate to locate access
18 credentials for said user;

19 returning, from said host access security system to said server machine, a user identifier
20 associated with said located access credentials and either a stored password or a generated
21 password substitute representing said located credentials;

22 modifying, by said server machine, said received log-on message by replacing said
23 placeholder syntax with said returned user identifier and password or password substitute; and

24 forwarding said modified log-on message from said server to said host system as a
25 response to said request for log-on information, such that said user identifier and password or
26 password substitute from said forwarded log-on message can be used by said host system to
27 transparently log said user on to a secure legacy host application executing at said host system,
28 without requiring change to said host system.

Claim 27 (canceled)

1 Claim 28 (previously presented): The method as claimed in Claim 26, wherein said digital
2 certificate is an X.509 certificate.

1 Claim 29 (currently amended): The method as claimed in Claim 26, wherein said communication

Serial No. 09/466,625

-8-

Docket RSW990077

2 protocol is a 3270 emulation legacy host communication protocol.

1 Claim 30 (currently amended): The method as claimed in Claim 26, wherein said communication
2 protocol is a 5250 emulation legacy host communication protocol.

1 Claim 31 (previously presented): The method as claimed in Claim 26, wherein said
2 communication protocol is a Virtual Terminal protocol.

1 Claim 32 (previously presented): The method as claimed in Claim 26, wherein said host access
2 security system is a Resource Access Control Facility (RACF) system.

1 Claim 33 (previously presented): A method of enabling a user at a client device to transparently
2 log on to a legacy session with a legacy host application, without requiring change to said legacy
3 host application, comprising steps of:

4 caching a digital certificate associated with said client device, or a user thereof, at a server
5 to which said digital certificate has been provided for authentication of said client device or said
6 user;

7 initiating, by said server on behalf of said client device, said legacy session with said legacy
8 host application;

9 automatically responding, by said client device, to a log-on request from said legacy host
10 application, where said log-on request is sent by said legacy host application responsive to said

11 initiating step, by sending a log-on message in which placeholder syntax is used in place of a user
12 identifier and password expected by said legacy host application; and
13 before forwarding said sent log-on message from said server to said legacy host
14 application, performing steps of:
15 using said cached digital certificate to obtain, at said server from a host access
16 security system, said expected user identifier and either said expected password or a password
17 substitute therefor which is generated by said host access security system; and
18 replacing said placeholder syntax in said sent log-on message with said obtained
19 user identifier and password or password substitute.

1 Claim 34 (new): The method as claimed in Claim 33, wherein said digital certificate is an X.509
2 certificate.

1 Claim 35 (new): The method as claimed in Claim 33, wherein said legacy session uses a 3270
2 legacy host communication protocol.

1 Claim 36 (new): The method as claimed in Claim 33, wherein said legacy session uses a 5250
2 legacy host communication protocol.

1 Claim 37 (new): The method as claimed in Claim 33, wherein said legacy session uses a Virtual
2 Terminal communication protocol.

1 Claim 38 (new): The method as claimed in Claim 33, wherein said host access security system is
2 a Resource Access Control Facility (RACF) system.

1 Claim 39 (new): A system for enabling a user at a client device to transparently log on to a legacy
2 session with a legacy host application, without requiring change to said legacy host application,
3 comprising:

4 means for caching a digital certificate associated with said client device, or a user thereof,
5 at a server to which said digital certificate has been provided for authentication of said client
6 device or said user;

7 means for initiating, by said server on behalf of said client device, said legacy session with
8 said legacy host application;

9 means for automatically responding, by said client device, to a log-on request from said
10 legacy host application, where said log-on request is sent by said legacy host application
11 responsive to said means for initiating, by sending a log-on message in which placeholder syntax is
12 used in place of a user identifier and password expected by said legacy host application; and

13 before forwarding said sent log-on message from said server to said legacy host
14 application, means for performing steps of:

15 using said cached digital certificate to obtain, at said server from a host access
16 security system, said expected user identifier and either said expected password or a password
17 substitute therefor which is generated by said host access security system; and

18 replacing said placeholder syntax in said sent log-on message with said obtained
19 user identifier and password or password substitute.

1 Claim 40 (new): The system as claimed in Claim 39, wherein said digital certificate is an X.509
2 certificate.

1 Claim 41 (new): The system as claimed in Claim 39, wherein said legacy session uses a 3270
2 legacy host communication protocol.

1 Claim 42 (new): The system as claimed in Claim 39, wherein said legacy session uses a 5250
2 legacy host communication protocol.

1 Claim 43 (new): The system as claimed in Claim 39, wherein said legacy session uses a Virtual
2 Terminal communication protocol.

1 Claim 44 (new): The system as claimed in Claim 39, wherein said host access security system is a
2 Resource Access Control Facility (RACF) system.

1 Claim 45 (new): A computer program product for enabling a user at a client device to
2 transparently log on to a legacy session with a legacy host application, without requiring change
3 to said legacy host application, said computer program product embodied on a computer-readable

4 medium readable by a computing device in a computing environment and comprising:

5 computer-readable program code means for caching a digital certificate associated with
6 said client device, or a user thereof, at a server to which said digital certificate has been provided
7 for authentication of said client device or said user;

8 computer-readable program code means for initiating, by said server on behalf of said
9 client device, said legacy session with said legacy host application;

10 computer-readable program code means for automatically responding, by said client
11 device, to a log-on request from said legacy host application, where said log-on request is sent by
12 said legacy host application responsive to said computer-readable program code means for
13 initiating, by sending a log-on message in which placeholder syntax is used in place of a user
14 identifier and password expected by said legacy host application; and

15 before forwarding said sent log-on message from said server to said legacy host
16 application, computer-readable program code means for performing steps of:

17 using said cached digital certificate to obtain, at said server from a host access
18 security system, said expected user identifier and either said expected password or a password
19 substitute therefor which is generated by said host access security system; and

20 replacing said placeholder syntax in said sent log-on message with said obtained
21 user identifier and password or password substitute.

1 Claim 46 (new): The computer program product as claimed in Claim 45, wherein said digital
2 certificate is an X.509 certificate.

1 Claim 47 (new): The computer program product as claimed in Claim 45, wherein said legacy
2 session uses a 3270 legacy host communication protocol.

1 Claim 48 (new): The computer program product as claimed in Claim 45, wherein said legacy
2 session uses a 5250 legacy host communication protocol.

1 Claim 49 (new): The computer program product as claimed in Claim 45, wherein said legacy
2 session uses a Virtual Terminal communication protocol.

1 Claim 50 (new): The computer program product as claimed in Claim 45, wherein said host access
2 security system is a Resource Access Control Facility (RACF) system.